



MyID
Version 11.5

SafeNet Network HSM Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | [@intercedemyid](https://twitter.com/intercedemyid) | +44 (0)1455 558111

Copyright

© 2001-2020 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

The software or web site referred to in this manual may utilize or contain material that is © 1994-2000 DUNDAS SOFTWARE LTD., all rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

Conventions Used in this Document

- Lists:
 - ♦ Numbered lists are used to show the steps involved in completing a task when the order is important
 - ♦ Bulleted lists are used when the order is unimportant or to show alternatives
- **Bold** is used for menu items and for labels.
For example:
 - ♦ “Record a valid email address in **‘From’ email address**”
 - ♦ Select **Save** from the **File** menu
- *Italic* is used for emphasis and to indicate references to other sections within the current document:
For example:
 - ♦ “Copy the file *before* starting the installation”
 - ♦ “See *Issuing a Card* for further information”
- ***Bold and italic*** are used to identify the titles of other documents.
For example: “See the ***Release Notes*** for further information.”
Unless otherwise explicitly stated, all referenced documentation is available on the installation media.
- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.
For example:
Note: This issue only occurs if updating from a previous version.
- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.
For example:

Warning: You must take a backup of your database before making any changes to it.

Contents

1	Introduction.....	5
1.1	What is an HSM?.....	5
1.2	What is needed?.....	5
1.3	SHA256 support	5
1.4	Supported SafeNet Network HSM models.....	5
1.5	Limitations.....	6
1.6	Multiple HSMs.....	6
1.7	HSM Test Utility	6
1.8	Previous version support	6
1.9	Change history.....	6
2	Installation and Configuration.....	7
2.1	Install HSM hardware and software	7
2.1.1	Installing SafeNet client software	8
2.2	Connecting to the HSM.....	8
2.2.1	Connecting to the HSM using PuTTY (versions 7.2 or earlier)	8
2.2.2	Connecting to the HSM (version 7.4 or later).....	10
2.3	Configure the SafeNet client software	10
2.4	Enabling strong protection	11
2.5	Configuring client version 7.....	11
2.6	Setting up the KSP	17
2.7	Test the connection	17
2.8	Protecting the Enrollment Agent, Key Recovery Agent, and PIV content signing certificates	17
2.8.1	Using KSP instead of CSP.....	18
2.9	Copy the SafeNet Network HSM PKCS#11 driver into System directory	18
2.10	Run GenMaster	18
2.11	Backup considerations.....	18
2.12	Installing older versions of client software	18
3	Troubleshooting	19

1 Introduction

This document provides a step-by-step guide to the configuration of MyID® to integrate with a SafeNet Network Hardware Security Module.

Note: If you have an existing installation of MyID and intend to change the HSM used with it, or want to migrate MyID database keys from the server registry or smart card to an HSM, contact Intercede customer support for further information quoting reference SUP-41.

1.1 What is an HSM?

A Hardware Security Module (referred to as an HSM) is a device that performs cryptographic operations on behalf of the host computer to which it is connected.

Offloading the cryptographic operations to a dedicated hardware device can have the following benefits:

- **Cryptographic acceleration**

Cryptographic operations (on which MyID heavily depends) can be processor-intensive. Carrying out these calculations on hardware that is optimized for them can improve performance and also leave the host computer's processor free to perform other tasks.

- **Improved Security**

Computers are general-purpose devices that can perform a wide variety of tasks. HSMs are specifically designed to store sensitive key data securely.

A computer stores its keys in its memory but an HSM has a dedicated memory store just used to store key data that is inaccessible to unauthorized access. It is often encased in a tamper-proof enclosure, or has built in security measures that will delete the sensitive key data if it is attacked.

Sensitive key data can be created as non-exportable, meaning that although the key can be used for cryptographic operations, it cannot be extracted or 'stolen'. An HSM is equivalent to a very high-performance server smartcard.

1.2 What is needed?

- Hardware requirements, supported platforms, and software requirements are specified in the [Installation and Configuration Guide](#). See the [Release Notes](#) for any late changes to these details.
- Documentation that is shipped with the SafeNet Network HSM should be read to identify any additional HSM-specific requirements.
- The SafeNet Network HSM administrator details (user account and password) – these may be the defaults or you may need to obtain them from the HSM administrator if your HSM facility is being hosted externally.

1.3 SHA256 support

MyID has been tested using SHA256 for the PIV server hash algorithm.

1.4 Supported SafeNet Network HSM models

MyID supports a network-based SafeNet Network HSM, connected using the SafeNet client software.

This HSM is also known as the Thales Trusted Cyber Technologies Luna HSM or the SafeNet Luna SA HSM.

1.5 Limitations

Currently, you cannot import AES192 keys encrypted by an AES transport key, or 3DES keys encrypted by an AES transport key. This is an issue with SafeNet firmware and will be addressed in a future firmware release.

As a workaround, for 3DES keys use another 3DES key as the transport key. For AES192 keys, either import into software rather than the HSM, or if possible use AES256 keys.

1.6 Multiple HSMs

MyID manages a connection to a single HSM. If you have more than one HSM set up for failover purposes, your HSM administrator must ensure that the data is synchronized between each HSM.

1.7 HSM Test Utility

A utility is provided with MyID to help confirm configuration with Hardware Security Modules (HSMs). This tool mimics the PKCS#11 transactions used by MyID and will exercise all functions of the HSM that MyID requires. You can use this utility to test cryptographic performance on the system; for example, to determine the optimum number of threads (concurrent operations) to achieve the best scalability for a given HSM.

You can find this utility in the `\Support Tools\HSM Integration\` folder on the MyID product media.

To set the number of HSM concurrent sessions, see the *HSM concurrency* section in the [Installation and Configuration Guide](#). This section also contains information on how to configure the number of retries for failed operations.

1.8 Previous version support

This manual documents how to set up a SafeNet Network HSM using the 7.0.0, 7.2, or 7.4 versions of the SafeNet client software. MyID also supports HSMs running previous firmware and client software.

Also, if your HSM uses a PIN Entry Device (PED), the procedure for setting up the new partition is different.

Contact customer support quoting reference SUP-230 for details of using MyID with older versions of the HSM firmware and client software.

1.9 Change history

Version	Description
INT1963-01	Released with MyID 11.0.
INT1963-02	Released with MyID 11.1.
INT1963-03	Released with MyID 11.2.
INT1963-04	Released with MyID 11.3.
INT1963-05	Released with MyID 11.4.
INT1963-06	Released with MyID 11.5.

2 Installation and Configuration

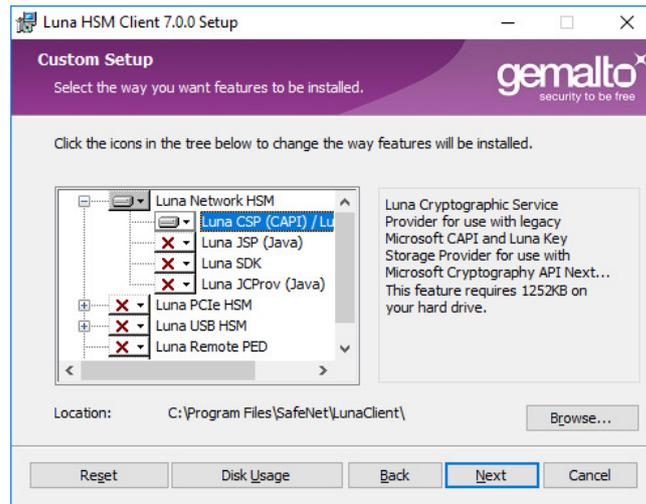
2.1 Install HSM hardware and software

1. Follow the instructions provided with the HSM to install the hardware and the SafeNet client software.

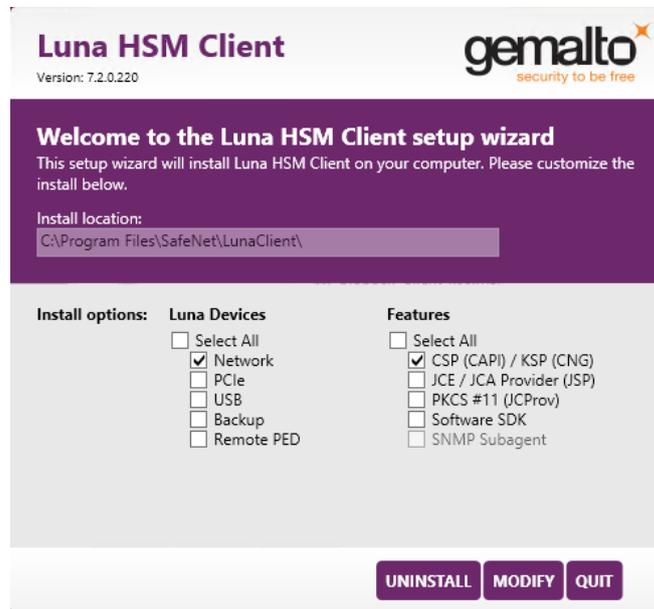
Install the client software on the MyID application server.

Note: Make sure you select the Luna CSP feature.

For SafeNet client software v7.1 or earlier:



For SafeNet client software v7.2 or v7.4:



2. Set up the HSM with a suitable administrator and network access.

2.1.1 Installing SafeNet client software

MyID is 32-bit software, and therefore requires the 32-bit version of the SafeNet software. The SafeNet client software is available as a 64-bit version only, but provides a 32-bit version of the `cryptoki.dll` file – see section 2.9, *Copy the SafeNet Network HSM PKCS#11 driver into System directory*.

The default installation location is:

```
C:\Program Files\SafeNet\LunaClient
```

2.2 Connecting to the HSM

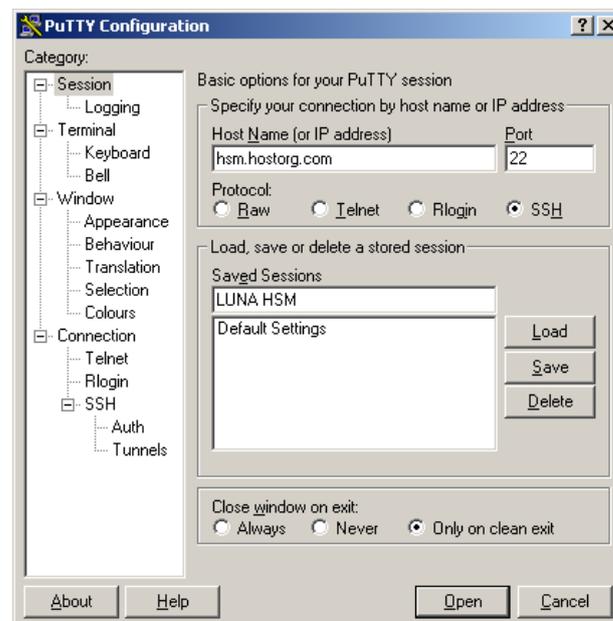
2.2.1 Connecting to the HSM using PuTTY (versions 7.2 or earlier)

Refer to the SafeNet documentation for your HSM for information on setting up the registration of the CSP.

1. Connect to the SafeNet HSM using SSH.

The `putty.exe` program supplied with the SafeNet client is located in the following folder:

```
C:\Program Files\SafeNet\LunaClient
```



The first time you use this program to connect to your HSM, you must:

- a) Specify the connection, as shown above, using appropriate information.
- b) Record an appropriate name in the **Saved Sessions** box and click **Save**.

To connect to the HSM:

- a) Highlight the connection information in the **Saved Sessions** list.
 - b) Click **Load**.
 - c) Click **Open**. A terminal window opens.
2. In the terminal window, log in to the HSM using the HSM `admin` account.

Note: If your HSM is being hosted externally, you will need to obtain the details for this from the host organization.

```
login as: admin
```

```
admin@lunasa01:
```

Last login: Tue May 24 21:20:46 2016 from 203.0.113.0

Luna SA 6.2.0-15 Command Line Shell - Copyright (c) 2001-2015
SafeNet, Inc. All rights reserved.

```
[lunasa01] lunash:>
```

3. Log in as the HSM administrator.

At the lunash:> prompt, type:

```
hsm login
```

Then type the HSM administrator password.

4. Create a new partition on the HSM for use by MyID.

At the lunash:> prompt, type:

```
partition create -name <partition name>
```

where <partition name> is the name you are using for the partition.

5. If multiple partitions are created, you will be able to select the appropriate partition when configuring MyID.

```
[lunasa01] lunash:>partition create -name MyPartition
```

Please ensure that you have purchased licenses for at least this
number of partitions: 8

If you have purchased licenses for at least this number of
partitions then type 'proceed', otherwise type 'quit'

```
> proceed
```

```
Proceeding...
```

```
Please enter a password for the partition:
```

```
> *****
```

```
Please re-enter password to confirm:
```

```
> *****
```

```
'partition create' successful.
```

```
Command Result : 0 (Success)
```

```
[lunasa01] lunash:>
```

2.2.2 Connecting to the HSM (version 7.4 or later)

For SafeNet client software version 7.4 or later, you do not use PuTTY; instead, the connection to the partition is set up automatically by running `lunacm.exe` (installed by the SafeNet client software to `C:\Program Files\SafeNet\LunaClient` by default). Within the Luna client window, enter the following command:

```
clientconfig deploy -server <server> -client <client> -partition
<partition> [-password <password>] [-user <user>] [-hsmPassword
<hsmpassword>] [-regen] [-force] [-verbose]
```

where:

- `-server` or `-n` – Server hostname or IP address (mandatory).
- `-client` or `-c` – Client hostname or IP address (mandatory).
- `-partition` or `-par` – Partition name to assign to the client (mandatory).
- `-password` or `-pw` – Appliance admin role user's password.
- `-user` or `-ur` – Appliance admin role user's name, default is admin.
- `-hsmPassword` or `-hsmPw` – HSM SO role password, only needed if HSM SO login enforcement is enabled.
- `-regen` or `-rg` – Regenerate new and replace existing client's certificate.
- `-force` or `-f` – Force Action.
- `-verbose` or `-v` – Show verbose logs.

For example:

```
clientconfig deploy -n myserver.safenet-inc.com -c myclient -par
mypartition -ur myuser -pw MyP4$$w0rd -v
```

2.3 Configure the SafeNet client software

The SafeNet client software needs to be told about the partitions on the HSM. Before you can do this, however, you must configure the client software to use 32-bit utilities in a 64-bit environment.

For more information, see the SafeNet Network HSM documentation.

To configure the SafeNet client software:

1. Copy the `crystoki.ini` file from the following 64-bit folder:
`C:\Program Files\SafeNet\LunaClient`
2. Copy the file into the following 32-bit folder:
`C:\Program Files\SafeNet\LunaClient\win32`
3. Open the copied `crystoki.ini` file (in the `win32` folder) in a text editor.
4. In the `[Crystoki2]` section, replace the old `LibNT` path with:
`LibNT=C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll`
5. For SafeNet client software 7 or earlier only:

In Windows, under **Computer>Properties>Advanced Settings>Environment Variables>System Variables**, set the following:

- ◆ `CrystokiConfigurationPath` – set the value to the following:
`C:\Program Files\SafeNet\LunaClient\win32`

Note: From SafeNet HSM client version 7.1, the `win32` subfolder is automatically appended to the path defined by the `ChrystokiConfigurationPath` system variable when using the 32-bit version of the client; this means that you must *not* modify the system variable.

To register the partition with the CSP software:

1. Log on to Windows as the MyID named COM user.
2. Right-click on the shortcut to the Windows **Command Prompt**, then from the pop-up menu select **Run as administrator**.

Change to the `C:\Program Files\SafeNet\LunaClient\Win32\CSP` folder.

3. Register the library; type:
`register /library`
4. Register the partition; type:
`register`
5. Accept all the following `[y/n]` prompts. For the challenge for partition, type the password for the partition.

Note: If your HSM uses a PIN Entry Device (PED), this is the partition password that was generated by the PED.

```
This procedure is a destructive procedure and will completely
replace any previous settings!!
```

```
Do you wish to continue?: [y/n]y
```

```
Do you want to register the partition named '2k8Test'?[y/n]: y
```

```
Enter challenge for partition '2k8Test' :*****
```

```
Success registering the ENCRYPTED challenge for partition
'2k8Test:1'.
```

```
Only the LunaCSP will be able to use this data!
```

```
Registered 1 partition(s) for use by the LunaCSP!
```

2.4 Enabling strong protection

MyID also supports the use of the `/strongprotect` option when registering the partition.

1. Register the partition with the `register` command, as in section [2.3, Configure the SafeNet client software](#).
2. Run each of your applications once to use Luna CSP.

You *must* configure and run each application that you want to use the Luna CSP. After you set the `/strongprotect` option, only users that have already accessed the CSP will be allowed to continue to access it.

For MyID, set the content signing certificates to use the CSP.

3. Run the register command again, with the `/strongprotect` option.

```
register /strongprotect
```

See the *CSP Registration Tool* documentation provided by SafeNet for more details.

2.5 Configuring client version 7

The SafeNet client software version 7 has the following major changes compared to previous version:

- How the trust connection between the HSM and MyID application server is configured.
- The introduction of a separation of duties concept for setting up the partition; there are now the following users involved in configuring the partition for use by MyID who can all have different passwords:
 - ♦ HSM Admin
 - ♦ HSM Security Officer
 - ♦ Partition Security Officer
 - ♦ Partition Crypto Officer – it is the partition crypto officer password which needs to be supplied to the P11 driver used by MyID.

You can connect to the HSM to help setup the trust connection; see [2.2, Connecting to the HSM](#)

[Connecting to the HSM](#) using PuTTY for details of connecting to the HSM using PuTTY.

To create the trust link between the client and the HSM:

1. On the MyID application server, open a Windows command prompt as an Administrator.
2. Navigate to the SafeNet utilities folder.

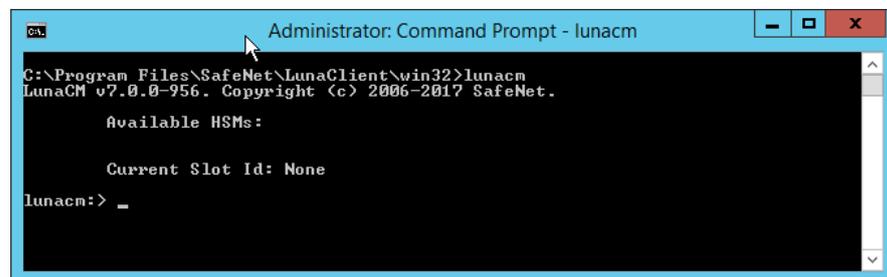
By default, this is:

```
C:\Program Files\SafeNet\LunaClient\win32
```

3. At the command prompt, type:

```
lunacm
```

This launches the command line environment that you will use to configure your connection to the HSM.



4. Establish the connection between the MyID application server and the HSM using the following command:

```
clientconfig deploy -server <hsm_ip> -client <app_ip> -partition <partition>
```

where:

- ♦ <hsm_ip> – the IP address of the HSM.
- ♦ <app_ip> – the IP address of the MyID application server.
- ♦ <partition> – the name of the partition you want to use.

```

Administrator: Command Prompt - lunacm
C:\Program Files\SafeNet\LunaClient\win32>lunacm
LunaCM v7.0.0-956. Copyright (c) 2006-2017 SafeNet.

Available HSMs:

Current Slot Id: None

lunacm:> clientconfig deploy -server 192.43.161.61 -client 80.2.227.81 -partitio
n elab1par19_
  
```

Press ENTER and wait for the command to complete.

5. When prompted, type the HSM admin password.

```

Administrator: Command Prompt - lunacm
C:\Program Files\SafeNet\LunaClient\win32>lunacm
LunaCM v7.0.0-956. Copyright (c) 2006-2017 SafeNet.

Available HSMs:

Current Slot Id: None

lunacm:> clientconfig deploy -server 192.43.161.61 -client 80.2.227.81 -partitio
n elab1par19
Please wait...

Using username "admin".
Please enter appliance admin role user's password: _
  
```

Press ENTER and wait for the command to complete.

```

Administrator: Command Prompt - lunacm
C:\Program Files\SafeNet\LunaClient\win32>lunacm
LunaCM v7.0.0-956. Copyright (c) 2006-2017 SafeNet

Available HSMs:

Current Slot Id: None

lunacm:> clientconfig deploy -server 192.43.161.61 -client 80.2.227.81 -partition elab1par19
Please wait...

Using username "admin".
Please enter appliance admin role user's password:
Last login: Thu Jan 11 09:44:03 2018 from 80.2.227.78

Luna SA 7.0.0-956 Command Line Shell - Copyright (c) 2001-2017 SafeNet, Inc. All rights reserved.

New server 192.43.161.61 successfully added to server list.

The following Luna SA Slots/Partitions were found:

Slot      Serial #      Label
====      =
0         1254270083762  Intercede

Command Result : No Error
lunacm:> _

```

If you see an error at this stage, possible causes are:

- ◆ You provided the wrong application server IP address.
 - ◆ The application server IP address is already registered on the HSM.
6. Close down `lunacm`: type `exit` and press ENTER.
 7. At the Windows command prompt, start `lunacm` again.

The `lunacm` utility displays the details of the HSM to which you are connected:

```

Administrator: Command Prompt - lunacm
C:\Program Files\SafeNet\LunaClient\win32>lunacm
LunaCM v7.0.0-956. Copyright (c) 2006-2017 SafeNet.

Available HSMs:

Slot Id -> 0
Label -> Intercede
Serial Number -> 1254270083762
Model -> LunaSA 7.0.0
Firmware Version -> 7.0.1
Configuration -> Luna User Partition With $0 <PW> Signing With C1
onging Mode
Slot Description -> Net Token Slot

Current Slot Id: 0

lunacm:> _

```

8. If you want to change to a different slot from the one listed, use the following command:

```
slot set -slot <slot_id>
```

where:

- ◆ `<slot_id>` – the number of the slot you want to use.

```

Administrator: Command Prompt - lunacm
Available HSMs:
Slot Id -> 0
Label -> Intercede
Serial Number -> 1254270083762
Model -> LunaS0 7.0.0
Firmware Version -> 7.0.1
Configuration -> Luna User Partition With SO <PW> Signing With Clonin
onning Mode
Slot Description -> Net Token Slot

Current Slot Id: 0
lunacm:> slot set -slot 0
Current Slot Id: 0 <Luna User Slot 7.0.1 <PW> Signing With Clonin
g Mode>
Command Result : No Error
lunacm:>

```

If the command completes successfully, `lunacm` displays:

Command Result : No Error

- To initialize the partition, use the following command:

```
partition init -label <label>
```

where:

- ◆ `<label>` – the label of the partition you want to initialize.

Follow the on-screen instructions. If the partition has already been initialized you will have to provide the existing SO password. If the partition has not been initialized, you must provide the partition domain.

```

Administrator: Command Prompt - lunacm
onning Mode
Slot Description -> Net Token Slot

Current Slot Id: 0
lunacm:> slot set -slot 0
Current Slot Id: 0 <Luna User Slot 7.0.1 <PW> Signing With Clonin
g Mode>
Command Result : No Error
lunacm:> partition init -label intercede

You are about to initialize the partition that is already initialized.
All contents of the partition will be destroyed.

You are required to provide the current Partition SO password.

Are you sure you wish to continue?

Type 'proceed' to continue, or 'quit' to quit now ->

```

Note: Make sure you take a note of the Partition SO password that you create.

If the command completes successfully, `lunacm` displays:

Command Result : No Error

- Log on to the initialized partition as the partition security officer using the following command:

```
role login -name po
```

- Type the password you entered when you initialized the partition.

```
Administrator: Command Prompt - lunacm
C:\Program Files\SafeNet\LunaClient\win32>lunacm
LunaCM v7.0.0-956. Copyright (c) 2006-2017 SafeNet.

Available HSMs:

Slot Id ->          0
Label ->            intercede
Serial Number ->   1254270003762
Model ->            LunaS0 7.0.0
Firmware Version -> 7.0.1
Configuration ->   Luna User Partition With S0 <PW> Signing With C1
Signing Mode
Slot Description -> Net Token Slot

Current Slot Id: 0

lunacm:> role login -name po

enter password: *****

Command Result : No Error

lunacm:> _
```

12. Initialize the crypto officer using the following command:

```
role init -name co
```

13. You are prompted to provide a new password.

Note: you are required to change this password before you can use the HSM with MyID; provide a temporary password.

```
Administrator: Command Prompt - lunacm

Available HSMs:

Slot Id ->          0
Label ->            intercede
Serial Number ->   1254270003762
Model ->            LunaS0 7.0.0
Firmware Version -> 7.0.1
Configuration ->   Luna User Partition With S0 <PW> Signing With C1
Signing Mode
Slot Description -> Net Token Slot

Current Slot Id: 0

lunacm:> role login -name po

enter password: *****

Command Result : No Error

lunacm:> role init -name co

enter new password: *****
re-enter new password: *****

Command Result : No Error

lunacm:> _
```

14. Change the crypto officer password.

You will be unable to use the HSM with MyID until you have changed the password. To confirm whether the crypto officer password needs to be changed:

- a) Log on to the HSM using PuTTY.

See section [2.2, Connecting to the HSM](#)

[Connecting to the HSM using PuTTY](#) for information on logging on to the HSM using PuTTY.

- b) Run the following command:

```
partition show -p <partition>
```

where:

- <partition> – the name of the partition you are using.

If the crypto officer password needs to be changed, the following text will appear in the report:

```
Crypto Officer          PIN To Be Changed:          yes
```

- c) If the report indicates that the crypto officer password needs to be changed:
 - i Open lunacm.
 - ii Log on as the crypto officer:


```
role login -name co
```
 - iii Change the password:


```
role changepw -name co
```
 - iv Follow the on-screen prompts.
- d) Use PuTTY again to connect to the HSM to confirm that the password does not need to be changed:


```
Crypto Officer          PIN To Be Changed:          no
```

2.6 Setting up the KSP

If you want to use the KSP for certificate templates, you must carry out some additional configuration.

Important: The username you specify in the `KspConfig.exe` tool must match the username used for the COM+ roles on the MyID application server; for example, if your MyID COM+ user is `MYDOMAIN\MyApp`, if you specify `MYDOMAIN\myapp` in the tool you will experience problems.

1. Locate the `KspConfig.exe` tool provided by SafeNet.

This tool is provided in both 32- and 64-bit versions. You must carry out the configuration with *both* versions of the tool.
2. Register the MyID COM+ user for the HSM slot using the **Slot Number** option.

Note: Do *not* use the default **Slot Label** option in the **Register By** group.

2.7 Test the connection

Test the PKCS#11 connection by starting the `ckdemo.exe` program in the `LunaSA` directory. It will not be able to complete `C_Initialize` if there is any communication problem with the HSM; if the program starts with no errors, the connection is working, and you can quit the program by entering option 0.

2.8 Protecting the Enrollment Agent, Key Recovery Agent, and PIV content signing certificates

You can protect your Enrollment Agent and Key Recovery Agent certificates using the HSM.

On PIV systems, you must also obtain a PIV content signing certificate. See the [PIV Integration Guide](#) for details.

You must log on to the application server using the MyID named COM user.

Make sure you use the 32-bit version of the Windows Certificate Manager:

```
C:\Windows\SysWOW64\certmgr.msc
```

When you request the certificates, you must change the Cryptographic Service Provider to select the CSP option **Luna enhanced RSA and AES provider for Microsoft Windows (Signature)**.

Make sure the **Export private keys** option is not selected.

2.8.1 Using KSP instead of CSP

MyID can use the KSP instead of the CSP for server certificates. See the following documents for details of setting up server certificates:

- [PIV Integration Guide](#) (for PIV Content Signer Certificate)
- [Microsoft Windows CA Integration Guide](#) (for Enrollment Agent and KRA certificates)
- [Mobile Identity Management Installation and Configuration Guide](#) (for mobile badge layout content signer certificate)
- [Smart Card Integration Guide](#) (for OPACITY signing certificate)

Note: You must configure the SafeNet KSP specifically for the MyID COM+ user account if the SafeNet KSP is to be used when issuing the CVC Signing Certificate for OPACITY.

- [Administration Guide](#) (for SCEP signing certificate)

2.9 Copy the SafeNet Network HSM PKCS#11 driver into System directory

Copy the file `cryptoki.dll` file from the `Program Files\SafeNet\LunaClient\win32` directory to the `Windows\SysWOW64` directory.

Warning: If you do not carry out this step, you cannot use the HSM in the GenMaster application to initialize the Keyserver database key.

2.10 Run GenMaster

As part of the MyID installation procedure, the GenMaster application is run to initialize the Keyserver database key. See the [Installation and Configuration Guide](#) for details.

Note: When you save the PIN for a SafeNet HSM using GenMaster, it is stored encrypted in the registry for the MyID COM+ user. If you want to update the PIN, or if you want to upgrade a previous installation to use an encrypted PIN, you can use the SetHSMPIN utility. See the [Setting the HSM PIN](#) section in the [Installation and Configuration Guide](#) for details.

2.11 Backup considerations

The cryptographic keys stored in the HSM are business critical data. If these keys are lost (for example, due to hardware failure) MyID will be unable to operate correctly and will lose the ability to manage issued devices.

You must create a backup strategy to protect the data in the HSM. If you generate any additional keys or import any additional keys, you must make sure your backup is up-to-date.

2.12 Installing older versions of client software

For instructions on installing clients earlier than version 7, or for instructions on setting up a SafeNet Network HSM with a PIN Entry Device (PED), contact customer support quoting reference SUP-230.

3 Troubleshooting

- **Error when HSM is not available**

If you attempt to activate a card at a time when the HSM is not available (for example, due to network problems) you may see an error similar to the following:

```
Applet Error
Command could not be processed
The Open Platform keys for this card are missing or incorrect. These
need to be corrected before issuance can continue.
-2147195391CEdeficeBOLException catch handler
Function : ProcessAPDUCommand, catch handler. Error :
Error: 0x80046601 : An Error occurred processing APDU commands for
the target Device
Info: Error performing ProtectedKey Crypto operation
Failure in ProtKeyCrypto Failure in external CryptoProvider module
0x80092004 Caught exception in CLUNAKeyServer::ProtKeyCrypto
Error: 0x80092004 : Cannot find object or property.
```

```
Info: Persisted key could not be found
-----
```

```
Exception raised in function: AbstractKeys::
P11SymmetricKey::FindPersistedKey
In file .\abstractkeys\P11SymmetricKey.cpp at line 351
-----
```

```
Exception raised in file .\ComFunctionObjects.cpp at line 928
```

If you experience this problem, contact Intercede customer support, quoting reference SUP-18.

- **Key server fails to start in HA mode when password is not cached**

On some MyID systems that were upgraded from MyID 8.0 and use an HSM in HA (cluster) mode when the partition PIN is not stored in the registry, the Key Server may fail to start with a message similar to:

```
Error in eKeySrv.SetKey
```

For more information, contact customer support, quoting reference SUP-174.

- **Safenet HSM Firmware 6.2.1 'small data encryption' problem**

A known issue exists in the HSM firmware version 6.2.1 that prevents certain operations involving 3DES/2DES/DES keys from succeeding. AES keys are unaffected by this problem.

If you are running HSM firmware version 6.2.1, you may experience errors in MyID when 3DES/2DES/DES keys are used.

When this problem occurs, the MyID workflow will fail, and errors will be logged in the MyID system events which contain the text:

```
Error: 0x00000030 : Device error
Info: Error Encrypting Data
```

or:

```
Error: 0x00000030 : Device error
Info: Error Decrypting Data
```

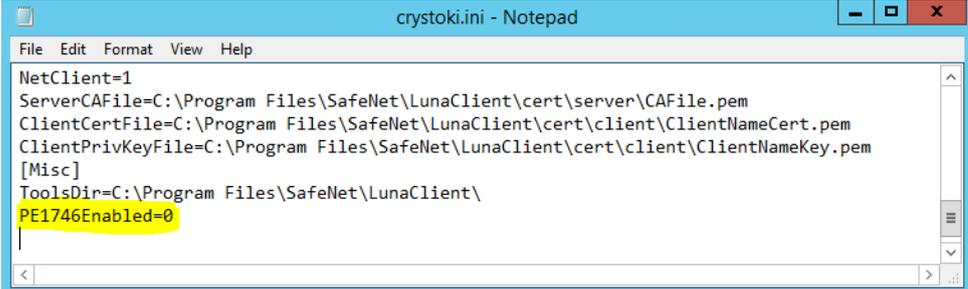
For Safenet HSM client software version 5.2 onwards, you can work around this problem by editing the `crystoki.ini` file.

Installations of Safenet HSM client software version 5.4.1 already have this workaround applied.

To apply the workaround:

- ◆ Edit the `crystoki.ini` file that is contained in the Safenet HSM installation on the MyID application server. Note that if multiple copies of `crystoki.ini` exist, you must apply the change to all copies.
- ◆ In the `[Misc]` section of `crystoki.ini`, ensure the setting `PE1746Enabled=0` is present.
- ◆ Reboot the MyID application server after the setting is changed.

Example `crystoki.ini` file with the workaround applied:



```
crystoki.ini - Notepad
File Edit Format View Help
NetClient=1
ServerCAFile=C:\Program Files\SafeNet\LunaClient\cert\server\CAFile.pem
ClientCertFile=C:\Program Files\SafeNet\LunaClient\cert\client\ClientNameCert.pem
ClientPrivKeyFile=C:\Program Files\SafeNet\LunaClient\cert\client\ClientNameKey.pem
[Misc]
ToolsDir=C:\Program Files\SafeNet\LunaClient\
PE1746Enabled=0
```